

# DIGITAL DATA RECORDING AND REPRODUCTION SYSTEM

Publication number: JP2001036523

Publication date: 2001-02-09

Inventor: KOMATA YOSHINOBU; KONDO TAKASHI

Applicant: OLYMPUS OPTICAL CO

Classification:

- international: G09C1/00; G06F21/00; G11B20/10; H04L9/32; H04N7/167; G09C1/00; G06F21/00; G11B20/10; H04L9/32; H04N7/167; (IPC1-7): H04L9/32; G09C1/00; G11B20/10; H04N7/167

- European: G06F21/00N1T; G06F21/00N3J5; G06F21/00N3P; G06F21/00N3P2; G06F21/00N5A2B; G06F21/00N5A2D; G06F21/00N9A2

Application number: JP19990207982 19990722

Priority number(s): JP19990207982 19990722

Also published as:

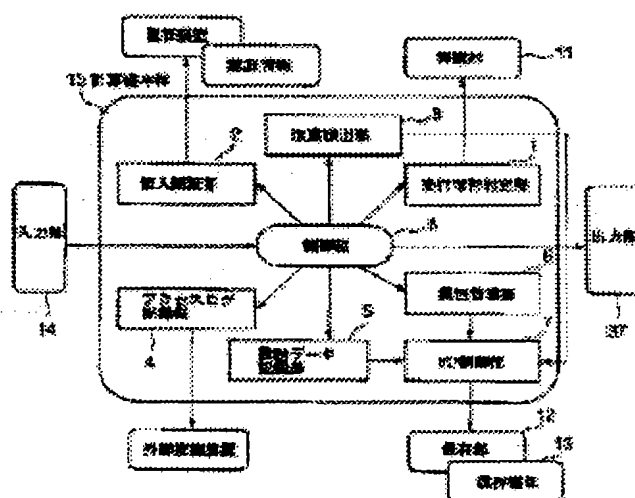
US6477530 (B1)

Report a data error here

## Abstract of JP2001036523

**PROBLEM TO BE SOLVED:** To obtain a system as a low cost data storage device that can be easily operated even when no network facility is available, by providing an execution propriety judging part to whether environment under which an operation control instruction is executed for each part is appropriate or not when operation control of each part is performed at a control part.

**SOLUTION:** Data inputted in a data input part 14 is handled so as to perform a specified processing including storage in a data storage part 12 as digital data in a computer main body 15 based on the operation control instruction by the control part 8 to each part provided with the data storage part 12 and the computer main body 15. When the digital data is outputted from a data output part 37 by responding to the request, the environment under which the operation control instruction by the control part 8 for each part is executed is appropriate or not by cooperation with a protecting part 11 connected with the computer main body 15 by the execution propriety judging part 1. A digital data recording and reproduction system is provided with the protecting part 11 to be connected with the computer main body 15.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-36523

(P2001-36523A)

(43) 公開日 平成13年2月9日 (2001.2.9)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコード <sup>*</sup> (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A 5 C 0 6 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 D 0 4 4
G 1 1 B 20/10		G 1 1 B 20/10	H 5 J 1 0 4
H 0 4 N 7/167		H 0 4 N 7/167	Z 9 A 0 0 1

審査請求 未請求 請求項の数14 O L (全 23 頁)

(21) 出願番号 特願平11-207982

(22) 出願日 平成11年7月22日 (1999.7.22)

(71) 出願人 000000376

オリンパス光学工業株式会社

東京都渋谷区幡ヶ谷2丁目43番2号

(72) 発明者 小俣 芳信

東京都渋谷区幡ヶ谷2丁目43番2号 オリ

ンパス光学工業株式会社内

(72) 発明者 近藤 隆

東京都渋谷区幡ヶ谷2丁目43番2号 オリ

ンパス光学工業株式会社内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外4名)

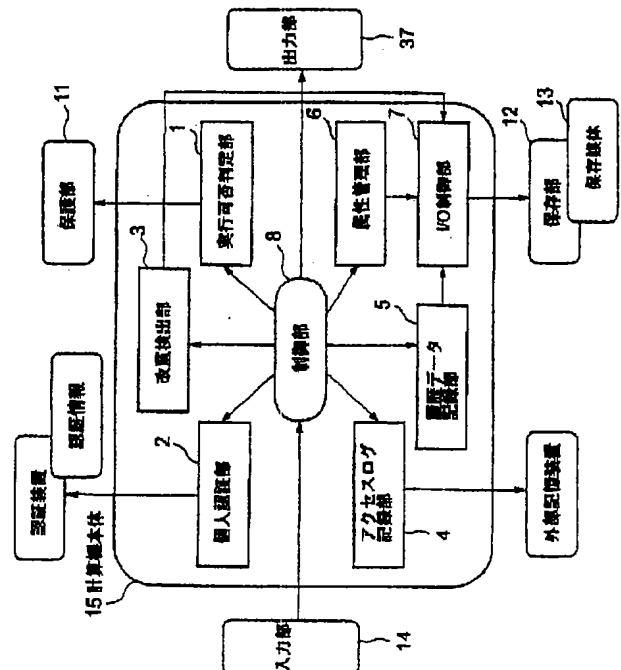
最終頁に続く

(54) 【発明の名称】 デジタルデータ記録再生システム

(57) 【要約】

【課題】本発明は、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供する。

【解決手段】本発明によると、データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体は、データ保存部と、個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうちの少なくとも一つと、前記データ保存部及び前記個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部とを備えることを特徴とする。



【特許請求の範囲】

【請求項1】 データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体は、デジタルデータを記憶するデータ保存部と、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部と、前記利用者が前記データ保存部に対してアクセスしたことを記録するアクセスログ記録部と、前記データ保存部に記憶されたデータが改竄されたか否かを検出する改竄検出部と、前記データ保存部に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部と、前記データ保存部に記憶されたデータの属性を管理する属性管理部とのうちの少なくとも一つと、前記データ保存部及び前記個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部と、を備えることを特徴とするデジタルデータ記録再生システム。

【請求項2】 前記デジタルデータ記録再生システムは、さらに、前記計算機本体に接続された保護部を備え、前記保護部は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を格納する読み出し専用不揮発性メモリとを備え、前記実行可否判定部は、前記保護部との通信により、前記読み出し専用不揮発性メモリに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項3】 前記実行可否判定部は、前記計算機本体に備えられた中央演算装置にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行なうことを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項4】 前記実行可否判定部は、複数の独立したホスト識別子読み取り部を備えたことを特徴とする請求項2記載のデジタルデータ記録再生システム。

【請求項5】 前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホ

スト識別子読み取り部であることを確認することを特徴とする請求項4記載のデジタルデータ記録再生システム。

【請求項6】 前記個人認証部は、認証情報が書き込まれたICカードと、前記ICカードに書き込まれた認証情報を読み取るICカード読取部とを備え、前記個人認証部とICカード読取部との間の通信に暗号化通信を用いることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項7】 前記個人認証部は、生体情報を入力するための生体情報入力部を備え、前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項8】 前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用電子署名と、を照合する照合部とを備えることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項9】 前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、を照合するための照合部とを備えることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項10】 前記アクセスログ記録部は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項11】 前記履歴データ記録部は、履歴データとして利用者を識別するための使用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項12】 前記制御部は、さらに、前記データ保存部内の保存媒体上のデータにアクセスするためのI/O制御部を備え、このI/O制御部は、前記保存媒体を識別するための保存媒体識別部と、データの情報を暗号化するための暗号化部と、暗号化されたデータを復号するための復号化部とを備えることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【請求項13】 前記暗号化部と復号化部は、それぞれ階層的な構造により暗号化レベルを変化することができることを特徴とする請求項12記載のデジタルデータ記録再生システム。

【請求項14】 前記属性管理部は、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを管理することを特徴とする請求項1記載のデジタルデータ記録再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータを保存するためのデジタルデータ記録再生システムに関し、例えば、光磁気ディスクなどの着脱可能でかつ書き換え可能な記録媒体にデジタルデータを保存するデジタルデータ記録再生システムに関する。

【0002】

【従来の技術】近年、パーソナルコンピュータなどの計算機の普及に伴い、各種の情報がデジタルデータとして記録媒体に保存されるようになってきている。

【0003】しかるに、計算機上で取り扱われるデジタルデータは、一般に、そのデータの複製、データの改竄などを容易に行うことができるので、データの保護やデータのセキュリティという観点からみると大きな問題となっている。

【0004】このような問題を解決するため、近時、公表されている「原本性保証電子保存システムの開発」

(創造的ソフトウェア育成事業及びエレクトリック・コマース推進事業に係る最終成果発表会1988)においては、2台の計算機をそれぞれ保存装置とホスト装置というように位置づけ、それらをLANなどのネットワークで接続して使用している。

【0005】ここで、保存装置とは、実際にデータが保存されている装置で、ネットワークコンピューティングの用語を使えば、サーバーといえることができる。

【0006】また、ホスト装置とは、ユーザが利用する端末の役割を果たし、ネットワークコンピューティングの用語を使えば、クライアントに相当する。

【0007】つまり、クライアント/サーバシステムをネットワーク上に構築することにより、データのアクセス方法に制約を加えることにより、データの機密性を高めるようにしている。

【0008】

【発明が解決しようとする課題】しかしながら、このようなデータ保存装置とホスト装置とによるクライアント/サーバシステムをネットワーク上に構築することは、少なくとも2台以上の計算機を必要とし、非常に高価なシステムになり導入時のコストが非常に高くなる点で問題となっている。

【0009】さらに、このようなデータ保存装置とホスト装置とによるクライアント/サーバシステムは、ネットワーク設備のない所では、運用することができないか、あるいは、ネットワーク設備からの導入が必要となるため、そのコストはさらに高くなるという問題がある。

【0010】本発明は、上記の事情に鑑みてなされたもので、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供することを目的とする。

【0011】

【課題を解決するための手段】本発明によると、上記課題を解決するために、(1) データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体は、デジタルデータを記憶するデータ保存部と、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部と、前記利用者が前記データ保存部に対してアクセスしたことを記録するアクセスログ記録部と、前記データ保存部に記憶されたデータが改竄されたか否かを検出する改竄検出部と、前記データ保存部に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部と、前記データ保存部に記憶されたデータの属性を管理する属性管理部とのうちの少なくとも一つと、前記データ保存部及び前記個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部と、を備えることを特徴とするデジタルデータ記録再生システムが提供される。

【0012】また、本発明によると、上記課題を解決するために、(2) 前記デジタルデータ記録再生システムは、さらに、前記計算機本体に接続された保護部を備え、前記保護部は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を格納する読み出し専用不揮発性メモリとを備え、前記実行可否判定部は、前記保護部との通信により、前記読み出し専用不揮発性メモリに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0013】また、本発明によると、上記課題を解決するために、(3) 前記実行可否判定部は、前記計算機本体に備えられた中央演算装置にあらかじめ書き込まれ

ている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行なうことを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0014】また、本発明によると、上記課題を解決するために、(4) 前記実行可否判定部は、複数の独立したホスト識別子読み取り部を備えたことを特徴とする(2)記載のデジタルデータ記録再生システムが提供される。

【0015】また、本発明によると、上記課題を解決するために、(5) 前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホスト識別子読み取り部であることを確認することを特徴とする(4)記載のデジタルデータ記録再生システムが提供される。

【0016】また、本発明によると、上記課題を解決するために、(6) 前記個人認証部は、認証情報が書き込まれたICカードと、前記ICカードに書き込まれた認証情報を読み取るICカード読取部とを備え、前記個人認証部とICカード読取部との間の通信に暗号化通信を用いることを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0017】また、本発明によると、上記課題を解決するために、(7) 前記個人認証部は、生体情報を入力するための生体情報入力部を備え、前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0018】また、本発明によると、上記課題を解決するために、(8) 前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用電子署名と、を照合する照合部とを備えることを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0019】また、本発明によると、上記課題を解決するために、(9) 前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、を照合するための照合部とを備えることを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0020】また、本発明によると、上記課題を解決するために、(10) 前記アクセスログ記録部は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0021】また、本発明によると、上記課題を解決するために、(11) 前記履歴データ記録部は、履歴データとして利用者を識別するための利用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0022】また、本発明によると、上記課題を解決するために、(12) 前記制御部は、さらに、前記データ保存部内の保存媒体上のデータにアクセスするためのI/O制御部を備え、このI/O制御部は、前記保存媒体を識別するための保存媒体識別部と、データの情報を暗号化するための暗号化部と、暗号化されたデータを復号するための復号化部とを備えることを特徴とする

(1)記載のデジタルデータ記録再生システムが提供される。

【0023】また、本発明によると、上記課題を解決するために、(13) 前記暗号化部と復号化部は、それぞれ階層的な構造により暗号化レベルを変化することができることを特徴とする(12)記載のデジタルデータ記録再生システムが提供される。

【0024】また、本発明によると、上記課題を解決するために、(14) 前記属性管理部は、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを管理することを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【0025】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。

【0026】図1は、本発明の一実施の形態として適用されるデジタルデータ記録再生システムの構成を示すブロック図である。

【0027】すなわち、図1に示すように、このデジタルデータ記録再生システムは、キーボード等の入力手段を含むデータ入力部14と、パーソナルコンピュータ(PC)等の計算機本体15と、ディスプレイ等の表示手段を含むデータ出力部37とからなり、前記データ入力部14により入力されたデータを前記計算機本体15内でデジタルデータとして取り扱うと共に、それを前記データ出力部37から出力するように構成されている。

【0028】このデジタルデータ記録再生システムにおいて、前記計算機本体15には、I/O制御部7を介してデジタルデータを記憶するデータ保存部12が接続されている。

【0029】そして、前記計算機本体15内には、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部2と、前記利用

者が前記データ保存部12に対してアクセスしたことを記録するアクセスログ記録部4と、前記データ保存部12に記憶されたデータが改竄されたか否かをI/O制御部7を介して検出する改竄検出部3と、前記データ保存部12に記憶されたデータに関する変更・修正情報をI/O制御部7を介して記録する履歴データ記録部5と、前記データ保存部12に記憶されたデータの属性をI/O制御部7を介して管理する属性管理部6とが備えられている。

【0030】また、この計算機本体15内には、前記データ保存部12及び前記個人認証部2、アクセスログ記録部4、改竄検出部3、履歴データ記録部5、属性管理部6の各々に対して動作命令を与えることにより、各部の動作制御を行う制御部8と、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定する実行可否判定部1とが備えられている。

【0031】また、デジタルデータ記録再生システムは、さらに、前記計算機本体15に接続された保護部11を備えている。

【0032】なお、図1では、デジタルデータを記憶するデータ保存部12は、I/O制御部7を介して計算機本体15に接続されている場合について説明したが、計算機本体15内に備えられていてもよい。

【0033】そして、このようなデジタルデータ記録再生システムでは、前記データ保存部12及び前記計算機本体15が備えている各部に対する前記制御部8による動作制御命令に基づいて、前記データ入力部14により入力されたデータを前記計算機本体15内でデジタルデータとしてデータ保存部12への保存を含む所定の処理を施すように取り扱うと共に、それを要求に応じて前記データ出力部37から出力する際に、前記実行可否判定部1が、前記計算機本体15に接続された保護部11との協働により、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定するようにしている。

【0034】ここで、実行可否判定部1は、前記計算機本体15に接続された保護部11との協働により、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境であると判定したときには前記計算機本体15による各部の処理を続行し、正当な環境でないと判定したときには前記計算機本体15による各部の処理が中止される。

【0035】ただし、実行可否判定部1は、前記計算機本体15で内部的に、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定することができる場合には、前記計算機本体15に接続された保護部11との協働を要しない。

【0036】なお、前記計算機本体15が備えている各部とは、前記個人認証部2、アクセスログ記録部4、改竄検出部3、履歴データ記録部5、属性管理部6のうち

の少なくとも一つを含むものとする。

【0037】従って、このようなデジタルデータ記録再生システムでは、従来の原本性保証電子保存システムのようにクライアント/サーバシステムをネットワーク上に構築することによってデータのアクセス方法に制約を加えることにより、データの機密性を高めるようにすることなく、簡易でしかも低コストで原本性保証電子保存システムとほぼ等価な機能が得られるようになるものである。

【0038】すなわち、以上のような図1の実施形態によると、データ入力部14と、計算機本体15と、データ出力部37とからなり、前記データ入力部14により入力されたデータを前記計算機本体15内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体15は、デジタルデータを記憶するデータ保存部12と、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部2と、前記利用者が前記データ保存部12に対してアクセスしたことを記録するアクセスログ記録部4と、前記データ保存部12に記憶されたデータが改竄されたか否かを検出する改竄検出部3と、前記データ保存部12に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部5と、前記データ保存部12に記憶されたデータの属性を管理する属性管理部6のうちの少なくとも一つと、前記データ保存部12及び個人認証部2、アクセスログ記録部4、改竄検出部3、履歴データ記録部5、属性管理部6のうち前記計算機本体15が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部8と、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部1とを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【0039】(実行可否判定部1による実行可否判定の具体例)次に、以上のような図1の実施形態における実行可否判定部1による実行可否判定の具体例について説明する。

【0040】(第1の具体例)図2は、実行可否判定部1による実行可否判定の第1の具体例を示す要部の構成図である。

【0041】図2に示すように、実行可否判定部1は、前記計算機本体15に接続された保護部11の読み出し専用不揮発性メモリ(EEPROM等)11aにあらかじめ格納されている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子16を取得することにより、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【0042】この場合、ホスト識別子16は、一意のデータである。

【0043】はじめに、実行可否判定部1は、前記計算機本体15のI/Oポートに接続されている保護部11に対してホスト識別子取得要求を送信する。

【0044】これに応じて、保護部11では、実行可否判定部1からのホスト識別子取得要求が正当なものと判断されたときには、実行可否判定部1に対して読み出し専用不揮発性メモリ11aにあらかじめ格納されているホスト識別子16を読み出して送信する。

【0045】このとき、実行可否判定部1と保護部11とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【0046】実行可否判定部1では、受信したホスト識別子16が正しい識別子であるか否かを判断し、このホスト識別子16が正しいと判定したときには前記計算機本体15による各部のときには処理を続行し、このホスト識別子16が正しくないと判定したときには前記計算機本体15による各部の処理が中止される。

【0047】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムは、さらに、前記計算機本体15に接続された保護部11を備え、前記保護部11は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子16を格納する読み出し専用不揮発性メモリ11aとを備え、前記実行可否判定部1は、前記保護部11との通信により、前記読み出し専用不揮発性メモリ11aに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とするデジタルデータ記録再生システムが提供される。

【0048】(第2の具体例)図3は、実行可否判定部1による実行可否判定の第2の具体例を示す要部の構成図である。

【0049】図3に示すように、実行可否判定部1は、前記計算機本体15に備えられている中央演算装置17にあらかじめ格納されているホスト識別子16を取得することにより、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【0050】この場合、ホスト識別子16は、例えば、製造時などに書き込まれる一意のデータである。

【0051】はじめに、実行可否判定部1は、前記計算機本体15に備えられている中央演算装置17に対してホスト識別子取得要求を送信する。

【0052】そして、中央演算装置17では、実行可否判定部1からのホスト識別子取得要求を受信すると、実行可否判定部1に対してホスト識別子16を送信する。

【0053】実行可否判定部1では、受信したホスト識別子16が正しい識別子であるか否かを判断し、このホスト識別子16が正しいと判定したときには前記計算機本体15による各部のときには処理を続行し、このホス

ト識別子16が正しくないと判定したときには前記計算機本体15による各部の処理が中止される。

【0054】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、前記計算機本体11に備えられた中央演算装置17にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子16を読み出して判定を行なうことを特徴とするデジタルデータ記録再生システムが提供される。

【0055】(第3の具体例)図4は、実行可否判定部1による実行可否判定の第3の具体例を示す要部の構成図である。

【0056】図4に示すように、n個のホスト識別子読み取り部a~n(18~20)を備えている実行可否判定部1は、前記計算機本体15に接続された保護部11の読み出し専用不揮発性メモリ11bにあらかじめ格納されている前記動作制御命令が実行される環境が正当な環境であることを保証するためのデータ列a~n(21~23)からなるホスト識別子16を取得することにより、前記動作制御命令を実行する環境が正当であるか否かを判断する。

【0057】この場合、データ列a~n(21~23)からなるホスト識別子16は、それぞれ、一意のデータである。

【0058】ここで、データ列a~nは、ホスト識別子16をn個に分割したもので、データ列aからデータ列bというようにデータ列nまでが順次結合されたとき、1つのホスト識別子を表すことができる。

【0059】はじめに、実行可否判定部1は、n個のホスト識別子読み取り部a~n(18~20)までを同時に起動する。

【0060】起動されたホスト識別子読み取り部18~20は、前記計算機本体15のI/Oポートに接続されている保護部11に対してホスト識別子16のデータ列21~23の取得要求を送信する。

【0061】このとき、実行可否判定部1では、各ホスト識別子読み取り部18~20に対して、あらかじめ、保護部11側のホスト識別子16のうちどのデータ列21~23を読み込むか指示しておくものとする。

【0062】保護部11では、ホスト識別子読み取り部18~20が、どのデータ列21~23の取得要求をしているのかに応じて、ホスト識別子読み取り部18~20に対応するデータ列21~23を読み出し専用不揮発性メモリ11bから読み出して送信する。

【0063】このとき、実行可否判定部1と保護部11とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【0064】ホスト識別子読み取り部18~20は、受信したデータ列21~23を直ちに実行可否判定手段1

に送信する。

【0065】実行可否判定手段1では、データ列21～23の再構成を行い、受信したホスト識別子16が正しい識別子であるか否かを判断し、このホスト識別子16が正しいと判定したときには前記計算機本体15による各部のときには処理を続行し、このホスト識別子16が正しくないと判定したときには前記計算機本体15による各部の処理が中止される。

【0066】このように、第3の具体例では、同時アクセスとデータ列の順番を入れ替えることにより、耐リバースエンジニアリング性能が高くなる。

【0067】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、複数の独立したホスト識別子読み取り部を備えたことを特徴とするデジタルデータ記録再生システムが提供される。

【0068】(第4の具体例)図5は、実行可否判定部1による実行可否判定の第4の具体例を示す要部の構成図である。

【0069】図5に示すように、n個のホスト識別子読み取り部a～n(18～20)を備えている実行可否判定部1は、前記計算機本体15に接続された保護部11の読み出し専用不揮発性メモリ11bにあらかじめ格納されているデータ列a～n(21～23)からなるホスト識別子16を取得することにより、前記動作制御命令を実行する環境が正当であるか否かを判断する。

【0070】この場合、ホスト識別子16は、前記動作制御命令を実行する環境が正当であることを保証するための、一意のデータである。

【0071】ここで、データ列a～nは、ホスト識別子16をn個に分割したもので、データ列aからデータ列bというようにデータ列nまでが順次結合されたとき、1つのホスト識別子を表すことができる。

【0072】はじめに、実行可否判定部1は、n個のホスト識別子読み取り部a～n(18～20)までを同時に起動する。

【0073】起動されたn個のホスト識別子読み取り部18～20は、各ホスト識別子読み取り部が正当なものであるか否かを確認するため、各ホスト識別子読み取り部18～20の間で通信を行う。

【0074】例えば、ホスト識別子読み取り部a(18)がホスト識別子読み取り部b(19)を確認するために、ホスト識別子読み取り部a(18)がホスト識別子読み取り部b(19)に識別コードA(24)を送信し、ホスト識別子読み取り部b(19)では、識別コードA(24)を受信してそれに対応する識別コードB(25)をホスト識別子読み取り部cに送るというように、最終的にホスト識別子読み取り部a(18)に適切なコードを受信することで各ホスト識別子読み取り部18～20の正当性を確認しあう。

【0075】すべての各ホスト識別子読み取り部18～20の正当性が確認されると、各ホスト識別子読み取り部18～20は、前記計算機本体15のI/Oポートに接続されている保護部11に対してホスト識別子16のデータ列21～23の取得要求を送信する。

【0076】このとき、実行可否判定部1では、各ホスト識別子読み取り部18～20に対して、あらかじめ、保護部11側のホスト識別子16のうちどのデータ列21～23を読み込むか指示しておくものとする。

【0077】保護部11では、ホスト識別子読み取り部18～20が、どのデータ列21～23の取得要求をしているのかに応じて、ホスト識別子読み取り部18～20に対応するデータ列21～23を読み出し専用不揮発性メモリ11bから読み出して送信する。

【0078】このとき、実行可否判定部1と保護部11とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【0079】ホスト識別子読み取り部18～20は、受信したデータ列21～23を直ちに実行可否判定手段1に送信する。

【0080】実行可否判定手段1では、データ列21～23の再構成を行い、受信したホスト識別子16が正しい識別子であるか否かを判断し、このホスト識別子16が正しいと判定したときには前記計算機本体15による各部のときには処理を続行し、このホスト識別子16が正しくないと判定したときには前記計算機本体15による各部の処理が中止される。

【0081】このように、第4の具体例では、同時アクセスとデータ列の順番を入れ替えることにより、耐リバースエンジニアリング性能が高くなる。

【0082】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホスト識別子読み取り部であることを確認することの特徴とするデジタルデータ記録再生システムが提供される。

【0083】(個人認証部2による個人認証の具体例)次に、以上のような図1の実施形態における個人認証部2による個人認証の具体例について説明する。

【0084】(第1の具体例)図6は、個人認証部2による個人認証の第1の具体例を示す要部の構成図である。

【0085】図7は、個人認証部2による個人認証の第1の具体例による個人認証手順を示すフローチャートである。

【0086】図6に示すように、個人認証部2は、ICカードリーダー31に挿入されたICカード32と通信することによって利用者の認証を行う。

【0087】図7に示すフローチャートに基づいてその認証手順を説明する。



【0088】はじめに、個人認証部2からICカードリーダー31を介してICカード32に対し、第1認証コード生成要求を送信する(ステップS1)。

【0089】ICカード32は、ICカードリーダー31を介して第1認証コード生成要求を受信して第1認証コードを生成し、それをICカードリーダー31を介して個人認証部2へ送信する(ステップS2)。

【0090】個人認証部2では、第1認証コードを受信すると、ICカード32内に格納されている内部認証キーを用いて所定の演算を行うことにより、第1応答コードを生成し、それをICカードリーダー31を介してICカード32へ送信する(ステップS3)。

【0091】ICカード32は、ICカードリーダー31を介して第1応答コードを受信すると、第1認証コードに対して外部認証キーを用いて所定の演算を行うことにより、第1応答コードとその計算結果とを比較する(ステップS4)。

【0092】続いて、ICカード32からICカードリーダー31を介して個人認証部2に対して、第2認証コード生成要求を送信する(ステップS5)。

【0093】個人認証部2は、第2認証コードを生成して、ICカードリーダー31を介してICカード32へ送信する(ステップS6)。

【0094】ICカード32では、ICカードリーダー31を介して第2認証コードを受信すると、ICカード32内に格納されている内部認証キーを用いて、所定の演算を行うことにより、第2応答コードを生成して、それをICカードリーダー31を介して個人認証部2へ送信する(ステップS6)。

【0095】個人認証部2は第2応答コードを受信すると、この第2認証コードに外部認証キーを用いて所定の演算を行うことにより、第2応答コードとその計算結果とを比較する(ステップS6)。

【0096】個人認証部2は、このような手順で計算結果を比較することにより、個人認証を行う。

【0097】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記個人認証部2は、認証情報が書き込まれたICカード32と、前記ICカードに書き込まれた認証情報を読み取るICカード読取部31とを備え、前記個人認証部2とICカード読取部31との間の通信に暗号化通信を用いることを特徴とするデジタルデータ記録再生システムが提供される。

【0098】(第2の具体例)図8は、個人認証部2による個人認証の第2の具体例を示す要部の構成図である。

【0099】図8に示すように、この第2の具体例によると、個人認証部2は、生体情報入力装置35と通信することによって利用者の認証を行う。

【0100】生体情報入力装置35は、光カード33に

書き込まれている生体情報36を読み取るための光カードリーダー31Aと生の生体情報を入力するための生体情報入力部34とにより構成される。

【0101】光カード33には、カード作成時にあらかじめ本人であることを保証する生体情報を、例えば、生の生体情報から照合に適した特徴量という形態に変換し、それをさらに暗号化して保存しておくものとする。

【0102】ここでは、生体情報として指紋を例にとつて、個人認証について説明する。

【0103】はじめに、個人認証部2が、出力部37に対して入力要請のメッセージ、例えば、「指を生体情報入力部へ置いて、ボタンを押して下さい」を表示する。

【0104】利用者がそのメッセージを見て指を生体情報入力部34に置き、ボタン34Aを押すと、生体情報入力部34での指紋のスキャンが始まり、この生体情報入力部34でスキャンされたデータが、個人認証部2へ送信される。

【0105】この生体情報入力部34でのスキャンが完了すると、光カードリーダー31Aに挿入された光カード33にあらかじめ本人であることを保証する生体情報として書き込まれている生体情報36が個人認証部2に送信される。

【0106】個人認証部2では、生体情報入力部34でスキャンされた生体情報の特徴量に変換するとともに、続いて光カード33から送られてきた生体情報36の復号化を行う。

【0107】そして、個人認証部2では、生体情報入力部34でスキャンされた生体情報の特徴量に変換したものと、光カード33から送られてきた生体情報36を照合することによって利用者が正当な利用者であるか否かの判定を行うことにより、利用者が正当な利用者である場合にのみ、当該システムの使用を許可する。

【0108】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記個人認証部は、生体情報を入力するための生体情報入力部を備え、前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とするデジタルデータ記録再生システムが提供される。

【0109】(改竄検出部3による改竄検出の具体例)次に、以上のような図1の実施形態における改竄検出部3による改竄検出の具体例について説明する。

【0110】(第1の具体例)図9は、改竄検出部3による改竄検出の第1の具体例を示す要部の構成図である。

【0111】図10は、改竄検出部3による改竄検出の第1の具体例による改竄検出手順を示すフローチャートである。

【0112】図9に示すように、改竄検出部3は、I/O制御手段7を介して、保存装置12に挿入された保存媒体13に保存されている各データ24の照合を行う照

合部3aを有している。

【0113】そして、この改竄検出部3の照合部3aは、利用者が保存媒体13に保存されている各データ24に対して修正や削除を行ったときに、それを検出するために機能するものである。

【0114】ここでは、利用者が保存媒体13に保存されているデータ1に対して修正を行った場合についての改竄検出手順を図10に示すフローチャートに基づいて説明する。

【0115】はじめに、改竄検出部3（の照合部3a）は、I/O制御手段7を通じて保存装置12に挿入されている保存媒体13のデータ24を読み出す（ステップS27）。

【0116】続いて、改竄検出部3（の照合部3a）は、この読み出されたデータ24に対する電子署名を算出する（ステップS28）。

【0117】ここで、電子署名はデータ24の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。

【0118】改竄検出部3（の照合部3a）は、電子署名の算出が終了すると、I/O制御手段7を介して、保存媒体13にデータ24が書き込まれたときに、それと共に書き込まれている電子署名25を読み出す（ステップS29）。

【0119】続いて、改竄検出部3（の照合部3a）は、計算された電子署名と保存媒体13より読み出された電子署名25との照合を行う（ステップS30）。

【0120】この場合、改竄検出部3（の照合部3a）は、計算された電子署名と保存媒体13より読み出された電子署名25との両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【0121】そして、改竄検出部3（の照合部3a）は、前記両者の照合結果として、両者が一致していた場合には、保存媒体13に保存されていたデータが改竄されていないことが保証され、両者が不一致の場合には、データが改竄されていることを検出する。

【0122】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部3は、前記計算機本体15に接続された保存部12の各データファイル（保存媒体13）に対して記録されている電子署名25と、前記保存部12の各データファイル（保存媒体13）から所定の算出式に基づいて計算される照合用電子署名と、を照合する照合部3aとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【0123】（第2の具体例）この第2の具体例において、改竄検出部3による改竄検出のを示す要部の構成は図9と同じである。

【0124】この第2の具体例において、改竄検出部3による改竄検出の手順は、図10に示すフローチャート

と同じである。

【0125】図9に示すように、改竄検出部3は、I/O制御手段7を介して、保存部12に挿入された保存媒体13に保存されているすべてのデータ24の照合を行う照合部3aを有している。

【0126】そして、この第2の具体例においては、利用者が保存媒体13を保存部12に挿入したときに、改竄検出部3（の照合部3a）が機能するものである。

【0127】ここでは、利用者が保存媒体13に保存されているデータ1に対して修正を行った場合についての改竄検出手順を図10に示すフローチャートに基づいて説明する。

【0128】はじめに、改竄検出部3（の照合部3a）は、I/O制御手段7を通じて保存部12に挿入されている保存媒体13のすべてのデータ24を読み出す（ステップS27）。

【0129】続いて、改竄検出部3（の照合部3a）は、この読み出されたデータ24に対する電子署名を算出する（ステップS28）。

【0130】ここで、電子署名はデータ24の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。

【0131】改竄検出部3（の照合部3a）は、電子署名の算出が終了すると、I/O制御手段7を介して、保存媒体13にデータ24が書き込まれたときに、それと共に書き込まれている電子署名25を読み出す（ステップS29）。

【0132】続いて、改竄検出部3（の照合部3a）は、計算された電子署名と保存媒体13より読み出された電子署名25との照合を行う（ステップS30）。

【0133】この場合、改竄検出部3（の照合部3a）は、計算された電子署名と保存媒体13より読み出された電子署名25との両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【0134】そして、改竄検出部3（の照合部3a）は、照合結果として、前記両者が一致していた場合には、保存媒体13に保存されていたデータが改竄されていないことが保証され、両者が不一致の場合には、データが改竄されていることを検出する。

【0135】なお、図9中の属性データ38は、後述する属性管理部6や履歴データ保存部5によって管理されるものである。

【0136】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部3は、前記計算機本体15に接続された保存部12の各データファイルに対して記録されている電子署名と、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、を照合するための照合部3aとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【0137】(履歴データ保存部5の具体例)次に、以上のような図1の実施形態における履歴データ保存部5の具体例について説明する。

【0138】図11は、履歴データ保存部5の具体例を示す要部の構成図である。

【0139】図11に示すように、履歴データ保存部5は、利用者が保存装置12に挿入されている保存媒体13に保存されている各データ24に対して修正や削除を行ったときに、属性データ38に履歴を追加する。

【0140】この履歴データ保存部5が管理する属性データ38は、図11では保存装置(保存部)12内に書き込むようにしているが、大容量の外部記憶装置がある場合には、その外部記憶装置に書き込むようにしても良い。

【0141】また、履歴データの内容は、利用者を識別するための使用者名を含むユーザーID、利用の日時を示すアクセス日時、利用者がどのような作業を行ったかを示すアクセス種別、使用した保存装置(保存部)12を特定するための保存装置識別子を含む保存装置のIDなどがある。

【0142】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記履歴データ記録部(保存部)5は、履歴データとして利用者を識別するための使用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする記載のデジタルデータ記録再生システムが提供される。

【0143】(アクセスログ記録部4の具体例)次に、以上のような図1の実施形態におけるアクセスログ記録部4の具体例について説明する。

【0144】図12は、アクセスログ記録部4の具体例を示す要部の構成図である。

【0145】図12に示すように、アクセスログ記録部4は、利用者が個人認証部2でシステムの使用が許可された場合、あるいはシステムの使用を終了したときにアクセスログを書き込む。

【0146】外部記憶装置12のアクセスログに対して、利用開始あるいは利用終了日時を含むアクセス日時、利用者を識別するための利用者名に対応したユーザー名、利用開始あるいは利用終了の種別を示すLogin/Logout、などのアクセス結果を書き込む。

【0147】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記アクセスログ記録部4は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とするデジタルデータ記録再生システムが提供される。

【0148】(属性管理部6の具体例)次に、以上のような図1の実施形態における属性管理部6の具体例について説明する。

【0149】図13は、属性管理部6の具体例を示す要部の構成図である。

【0150】図13に示すように、属性管理部6は、利用者がデータのステータスの変更を行ったときに、属性データ38の更新を行う。

【0151】この属性データ38の内容は、ファイル名、データの内容がファイルであるのかディレクトリであるのか識別するためのファイルタイプ、ファイルのサイズ、ファイルへのアクセス制限を示すファイルアトリビュート、ファイルが原本ファイル、仮原本ファイル、謄本ファイル、一般ファイルの区別をするためのファイルステータス、ファイルの作成者、ファイルの作成日時、ファイルの更新者、ファイルの更新日時、保存期間などがあり、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを含む。

【0152】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記属性管理部6は、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを管理することを特徴とするデジタルデータ記録再生システムが提供される。

【0153】(I/O制御部7の具体例)次に、以上のような図1の実施形態におけるI/O制御部7の具体例について説明する。

【0154】(第1の具体例)図14は、I/O制御部7の第1の具体例を示す要部の構成図である。

【0155】図14に示すように、I/O制御部7は、保存装置(保存部)12に挿入された保存媒体13のデータの入出力手順を規定する。

【0156】例えば、利用者が保存媒体13へアクセスしようとするとき、はじめに、I/O制御部7内の媒体種別判定部39は、保存装置(保存部)12に挿入されている保存媒体13が専用保存媒体かあるいは一般保存媒体であるか判断する。

【0157】そして、保存媒体13が専用保存媒体である場合には、I/O制御部7内の第1暗号化/復号化部40を介してデータの入出力を行う。

【0158】まず、利用者が保存媒体13へデータの書き込みを行うと、第1暗号化/復号化部40は、暗号化部として働き、ここを通過するデータを所定の手続きにより暗号化する。

【0159】また、利用者が保存媒体13からデータの読み出しを行うと、第1暗号化/復号化部40は、復号化部として働き、ここを通過するデータを所定の手続き

により復号化する。

【0160】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記制御部8は、さらに、前記データ保存部12内の保存媒体13上のデータにアクセスするためのI/O制御部7を備え、このI/O制御部7は、前記保存媒体を識別するための保存媒体識別部39と、データの情報を暗号化するための暗号化部40と、暗号化されたデータを復号するための復号化部40とを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【0161】(第2の具体例)図15は、I/O制御部7の第2の具体例を示す要部の構成図である。

【0162】図15に示すように、I/O制御部7は、保存装置12に挿入された保存媒体13のデータの出入力手順を規定する。

【0163】例えば、利用者が保存媒体13へアクセスしようとするとき、はじめに、I/O制御部7内の媒体種別判定部39は、保存装置12に挿入されている保存媒体13が専用保存媒体かあるいは一般保存媒体であるか判断する。

【0164】そして、保存媒体13が専用保存媒体である場合には、階層的に構成されたI/O制御部7内の第1暗号化/復号化部40から第n暗号化/復号化部41を介してデータの出入力を行う。

【0165】まず、利用者が保存媒体13へデータの書き込みを行うと、第1暗号化/復号化部40は、第1暗号化部として働き、ここを通過するデータを所定の手続きにより暗号化すると共に、そのデータを第2暗号化/復号化部へと送る。

【0166】第2暗号化/復号化部も、第1暗号化/復号化部40と同様に、暗号化部として働き、そこを通過するデータを所定の手続きにより暗号化するというように、以下、n階層の暗号化/復号化部を介してデータの書き込みを行う。

【0167】また、利用者が保存媒体13からデータの読み出しを行うと、第1暗号化/復号化部40は、第1復号化部として働き、ここを通過するデータを所定の手続きにより復号化すると共に、そのデータを第2暗号化/復号化部へと送る。

【0168】第2暗号化/復号化部も、第1暗号化/復号化部40と同様に、復号化部として働き、そこを通過するデータを所定の手続きにより復号化するというように、以下、n階層の暗号化/復号化部を介してデータの復号化を行う。

【0169】このように、I/O制御部7の第2の具体例では、暗号化を階層的に行うことにより、データの機密性を高くすることができる。

【0170】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記暗号化部40と復号化部40は、それぞれ階層的な構造に

より暗号化レベルを変化することができることを特徴とするデジタルデータ記録再生システムが提供される。

【0171】(システム起動の具体例)次に、以上のような図1の実施形態におけるシステム起動の具体例について説明する。

【0172】図16は、システム起動の具体例を示す要部のフローチャートである。

【0173】図16に示すように、利用者により実行処理開始が入力部14より指示される(ステップS42)と、制御部8内の復号化部は、所定の暗号化方式により暗号化された各部を復号し、実行可能状態にする(ステップS43)。

【0174】続いて、実行可否判定部1によって、各部の実行環境が正当であるか否かが判断され(ステップS44)、正当である場合には制御部8が起動されて起動状態になるが、正当でない場合には、起動されない。

【0175】(システム終了の具体例)次に、以上のような図1の実施形態におけるシステム終了の具体例について説明する。

【0176】図17は、システム終了の具体例を示す要部のフローチャートである。

【0177】図17に示すように、すべての処理が終了し、利用者により終了処理開始46が実行される(ステップS46)と、制御部8内の終了部が実行され、制御部8が終了する(ステップS47)。

【0178】制御部8が終了すると同時に、制御部8内の暗号化部が実行され、制御部8が暗号化されることにより(ステップS48)、実行不可能状態になって終了する(ステップS49)。

【0179】(新規データ登録処理の具体例)次に、以上のような図1の実施形態における新規データ登録処理の具体例について説明する。

【0180】図18は、新規データ登録処理についての具体例を示す要部のフローチャートである。

【0181】図18に示すように、新規登録処理開始が実行される(ステップS50)と、正当な利用者であるか確認するため、個人認証部2で利用者の認証確認が行われる(ステップS51)。

【0182】図18では毎回、認証を行うように記しているが一度、認証を行えば2回目以降は認証を行う必要はない。

【0183】続いて、利用者の情報を記録するため、アクセスログ記録部4での処理が実行される(ステップS52)。

【0184】続いて、新規に登録するデータの属性の情報を記録するため属性管理部6での処理が実行される(ステップS53)。

【0185】続いて、データの履歴情報を記録するため履歴データ記録部5での処理が実行される(ステップS54)。

【0186】続いて、データの保存媒体13への書き込みが行われ（ステップS55）、書き込みが行われたデータに対する電子署名を作成する処理が実行され（ステップS56）た後、新規登録処理を終了する（ステップS57）。

【0187】図18では、属性管理部6での処理、履歴データ記録部5での処理、保存媒体13への書き込み、電子署名作成の順番で処理を行うように記してあるが、これらの実行順序は問わない。

【0188】（登録データの更新の具体例）次に、以上のような図1の実施形態における登録データの更新の具体例について説明する。

【0189】図19は、登録データの更新の具体例を示す要部のフローチャートである。

【0190】図19に示すように、登録データ更新処理開始が実行される（ステップS58）と、正当な利用者であるか確認するため、個人認証部2で利用者の認証確認が行われる（ステップS59）。

【0191】図19では毎回、認証を行うように記しているが一度、認証を行えば2回目以降は認証を行う必要はない。

【0192】続いて、利用者の情報を記録するため、アクセスログ記録部4での処理が実行される（ステップS60）。

【0193】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部3での処理が実行される（ステップS61）。

【0194】改竄検出部3によりデータの書き換え、変更がなされていることが確認されると、改竄通知が実行され（ステップS62）、利用者にデータの書き換え、変更がなされていることを通知して更新を行うことなく処理を終了する（ステップS63）。

【0195】改竄検出部3において、データの書き換え、変更が行われていないことが確認された場合には、更新するデータの属性の情報を記録するため属性管理部6での処理が実行される（ステップS64）。

【0196】続いて、データの履歴情報を記録するため履歴データ記録部5での処理が実行される（ステップS65）。

【0197】続いて、データの保存媒体13への書き込みが行われ（ステップS66）、書き込みが行われたデータに対する電子署名を作成する処理が実行され（ステップS67）た後、登録データ更新処理を終了する（ステップS68）。

【0198】図19では、属性管理部6での処理、履歴データ記録部5での処理、保存媒体13への書き込み、電子署名作成の順番で処理を行うように記してあるが、これらの実行順序は問わない。

【0199】（登録データの削除の具体例）次に、以上

のような図1の実施形態における登録データの削除の具体例について説明する。

【0200】図20は、登録データの削除の具体例を示す要部のフローチャートである。

【0201】図20に示すように、登録データ削除処理開始が実行される（ステップS69）と、正当な利用者であるか確認するため、個人認証部2で利用者の認証確認が行われる（ステップS70）。

【0202】図20では毎回、認証を行うように記しているが一度、認証を行えば2回目以降は認証を行う必要はない。

【0203】続いて、利用者の情報を記録するため、アクセスログ記録部4での処理が実行される（ステップS71）。

【0204】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部3での処理が実行される（ステップS72）。

【0205】改竄検出部3によりデータの書き換え、変更がなされていることが確認されると、改竄通知が実行され（ステップS73）、利用者にデータの書き換え、変更がなされていることを通知して削除を行うことなく処理を終了する（ステップS74）。

【0206】改竄検出部3において、データの書き換え、変更が行われていないことが確認された場合には、保存媒体13に登録されているデータのうち削除するデータの削除が行われる（ステップS75）。

【0207】続いて、その削除データの属性の情報を記録したデータ、電子署名が削除が行われる。（ステップS76）。

【0208】（登録データの複製の具体例）次に、以上のような図1の実施形態における登録データの複製の具体例について説明する。

【0209】図21は、登録データの複製の具体例を示す要部のフローチャートである。

【0210】図21に示すように、登録データ複製処理開始が実行される（ステップS77）と、正当な利用者であるか確認するため、個人認証部2で利用者の認証確認が行われる（ステップS78）。

【0211】図21では毎回、認証を行うように記しているが一度、認証を行えば2回目以降は認証を行う必要はない。

【0212】続いて、利用者の情報を記録するため、アクセスログ記録部4での処理が実行される（ステップS79）。

【0213】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部3での処理が実行される（ステップS80）。

【0214】改竄検出部3によりデータの書き換え、変

更がなされていることが確認されると、改竄通知が実行され（ステップS81）、利用者にデータの書き換え、変更がなされていることを通知して複製を行うことなく処理を終了する（ステップS82）。

【0215】改竄検出部3においてデータの書き換え、変更が行われていないことが確認された場合には、データの属性確認を行うため属性確認部6での処理が実行される（ステップS83）。

【0216】データを複製するには、複製（作成）元データが原本である必要があるため、データの属性の確認を行うものであって、作成元データが原本でない場合には複製の作成を行うことができないので、複製を行うことなく処理を終了する（ステップS82）。

【0217】しかるに、複製（作成）元データが原本である場合には、複製（作成）元データの属性の情報を記録するために、属性管理部6での処理が実行される（ステップS84）。

【0218】続いて、データの履歴情報を記録するため履歴データ記録部5での処理が実行される（ステップS85）。

【0219】続いて、データの保存媒体13への書き込みが行われ（ステップS86）、書き込みが行われたデータに対する電子署名を作成処理が実行され（ステップS87）た後、複製（作成）元データの属性の情報を記録するために、属性管理部6での処理が実行される（ステップS88）。

【0220】続いて、データの履歴情報を記録するために、履歴データ記録部5での処理が実行される（ステップS89）た後、登録データ複製処理を終了する（ステップS90）。

【0221】

【発明の効果】従って、以上説明したように、本発明によれば、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供することができる。

【図面の簡単な説明】

【図1】図1は、本発明の一実施の形態として適用されるデジタルデータ記録再生システムの構成を示すブロック図である。

【図2】図2は、図1の実行可否判定部1による実行可否判定の第1の具体例を示す要部の構成図である。

【図3】図3は、図1の実行可否判定部1による実行可否判定の第2の具体例を示す要部の構成図である。

【図4】図4は、図1の実行可否判定部1による実行可否判定の第3の具体例を示す要部の構成図である。

【図5】図5は、図1の実行可否判定部1による実行可否判定の第4の具体例を示す要部の構成図である。

【図6】図6は、図1の個人認証部2による個人認証の第1の具体例を示す要部の構成図である。

【図7】図7は、図1の個人認証部2による個人認証の第1の具体例による個人認証手順を示すフローチャートである。

【図8】図8は、図1の個人認証部2による個人認証の第2の具体例を示す要部の構成図である。

【図9】図9は、図1の改竄検出部3による改竄検出の第1の具体例を示す要部の構成図である。

【図10】図10は、図1の改竄検出部3による改竄検出の第1の具体例による改竄検出手順を示すフローチャートである。

【図11】図11は、図1の履歴データ保存部5の具体例を示す要部の構成図である。

【図12】図12は、図1におけるアクセスログ記録部4の具体例を示す要部の構成図である。

【図13】図13は、図1の属性管理部6の具体例を示す要部の構成図である。

【図14】図14は、図1におけるI/O制御部7の第1の具体例を示す要部の構成図である。

【図15】図15は、図1におけるI/O制御部7の第2の具体例を示す要部の構成図である。

【図16】図16は、図1におけるシステム起動の具体例を示す要部のフローチャートである。

【図17】図17は、図1におけるシステム終了の具体例を示す要部のフローチャートである。

【図18】図18は、図1のシステムにおける新規データ登録処理についての具体例を示す要部のフローチャートである。

【図19】図19は、図1のシステムにおける登録データの更新の具体例を示す要部のフローチャートである。

【図20】図20は、図1のシステムにおける登録データの削除の具体例を示す要部のフローチャートである。

【図21】図21は、図1のシステムにおける登録データの複製の具体例を示す要部のフローチャートである。

【符号の説明】

14…データ入力部、

15…計算機本体、

37…データ出力部、

7…I/O制御部、

12…データ保存部、

13…保存媒体、

2…個人認証部、

4…アクセスログ記録部、

3…改竄検出部、

5…履歴データ記録部、

6…属性管理部、

8…制御部、

1…実行可否判定部、

11…保護部、

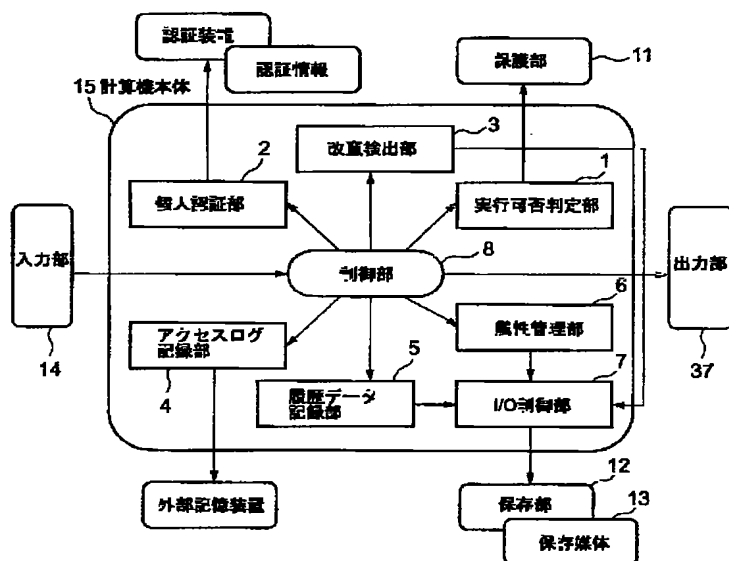
11a, 11b…読み出し専用不揮発性メモリ、

16…ホスト識別子、

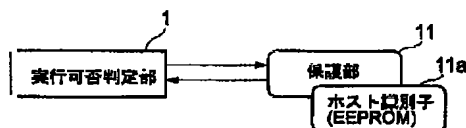
17…中央演算装置、  
 18～20… $n$ 個のホスト識別子読み取り部 $a \sim n$ 、  
 21～23データ列、  
 24…データ、  
 25…電子署名、  
 31…ICカードリーダ、  
 32…ICカード、  
 35…生体情報入力装置、  
 34…生体情報入力部、

34A…ボタン、  
 33…光カード、  
 31A…光カードリーダ部、  
 36…生体情報、  
 3a…照合部、  
 38…属性データ、  
 39…媒体種別判定部、  
 40…第1暗号化/復号化部、  
 41…第 $n$ 暗号化/復号化部。

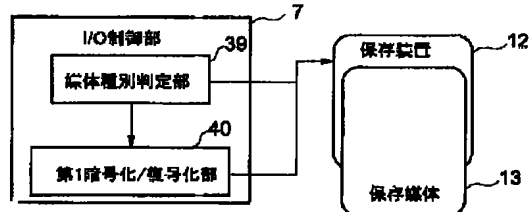
【図1】



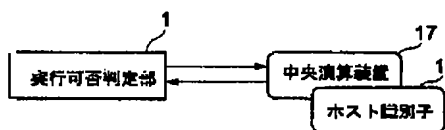
【図2】



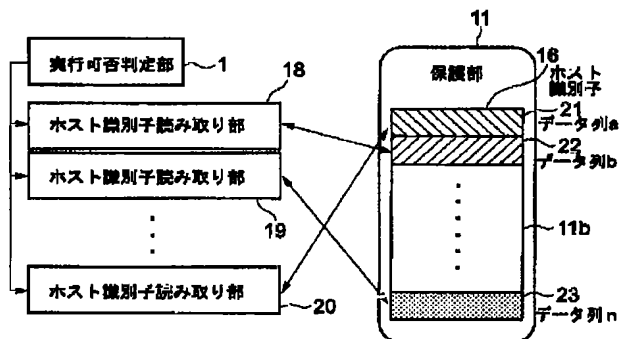
【図14】



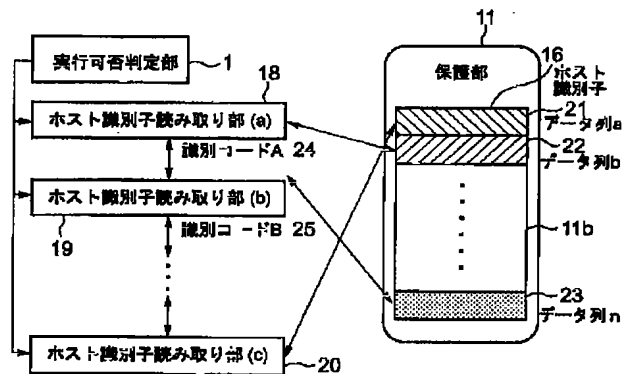
【図3】



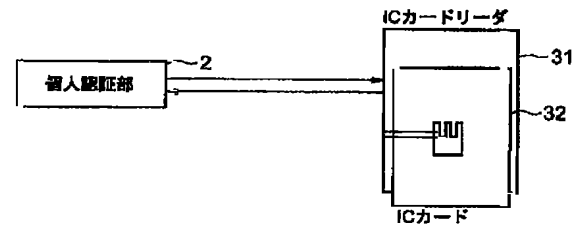
【図4】



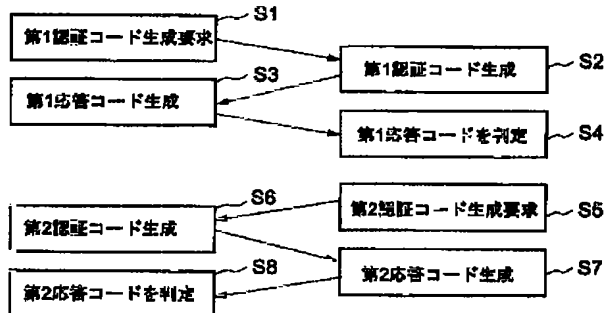
【図5】



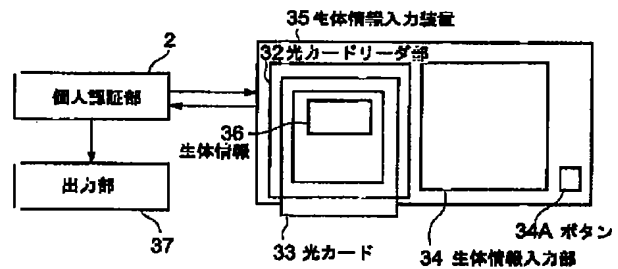
【図6】



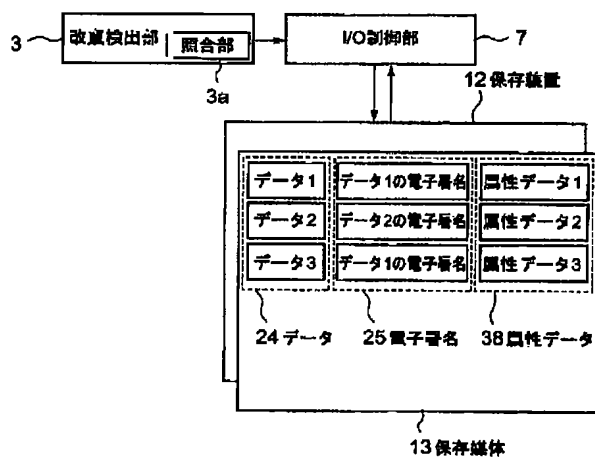
【図7】



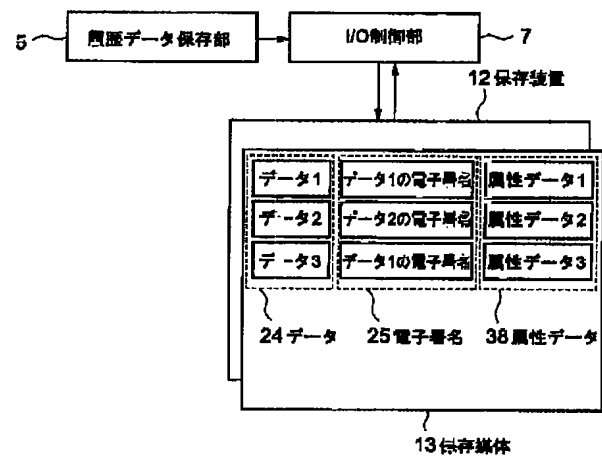
【図8】



【図9】

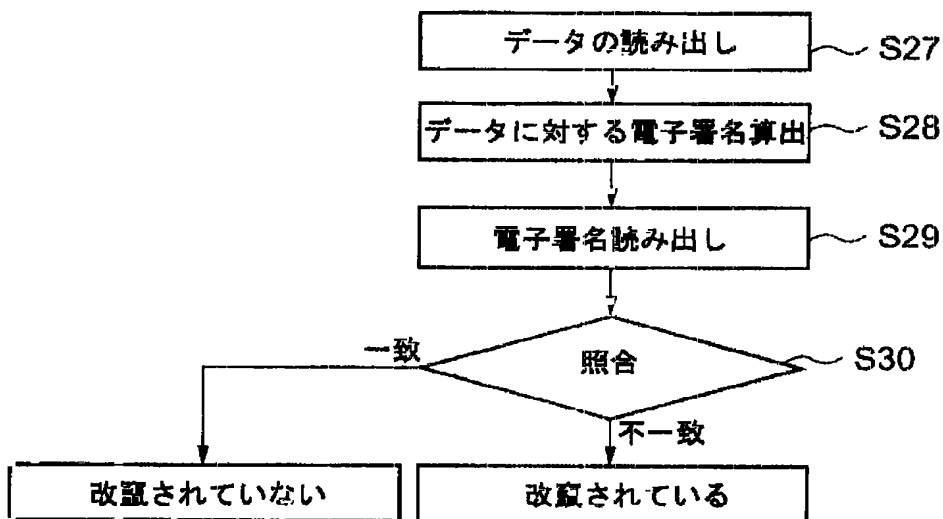


【図11】

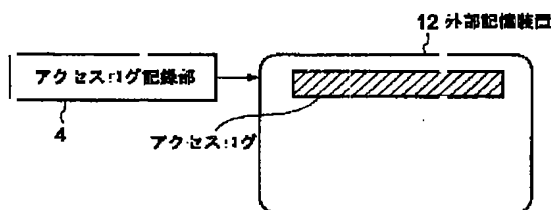




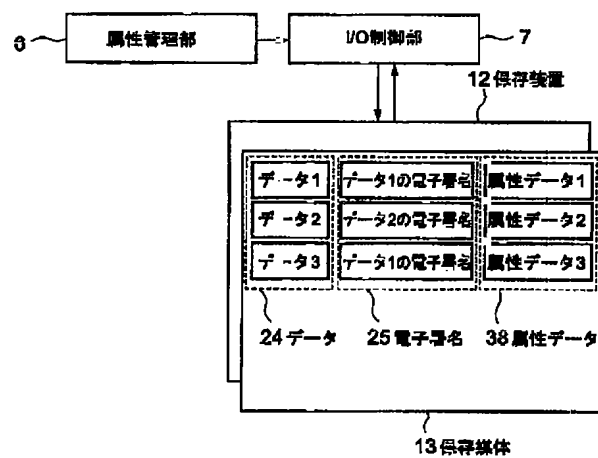
【図10】



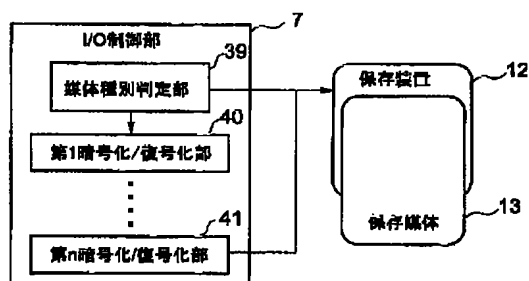
【図12】



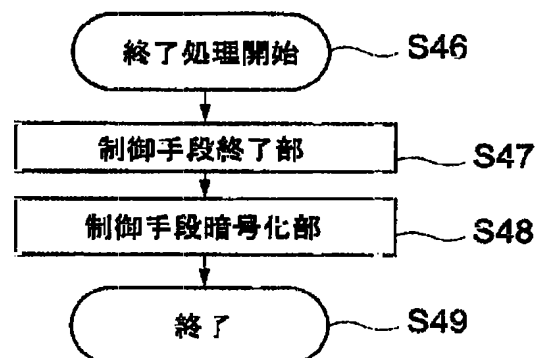
【図13】



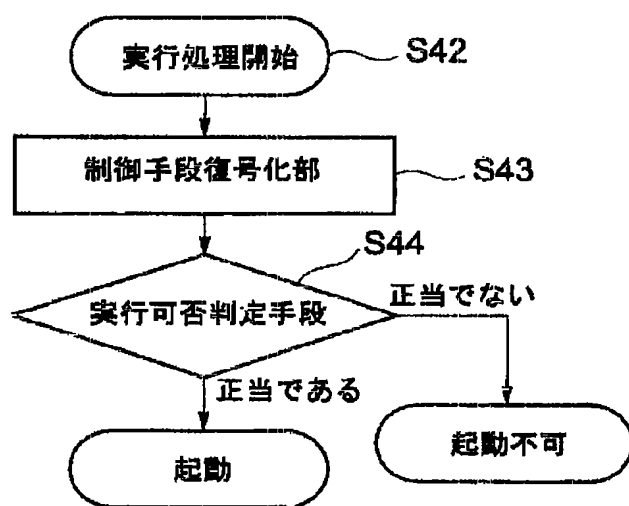
【図15】



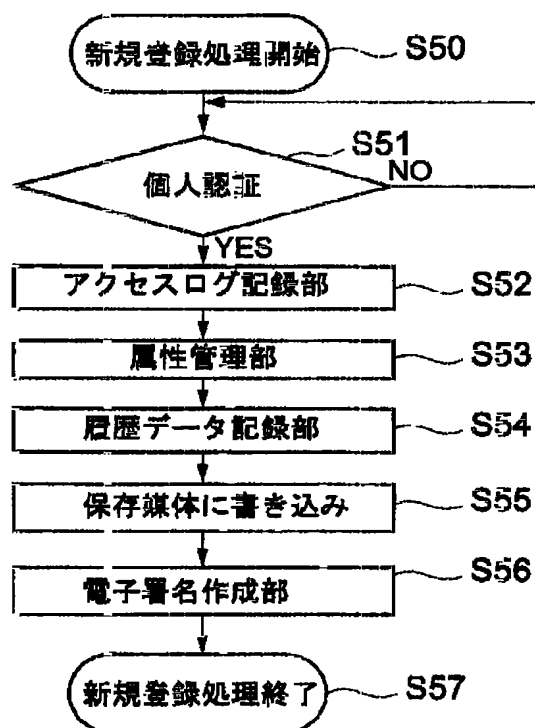
【図17】



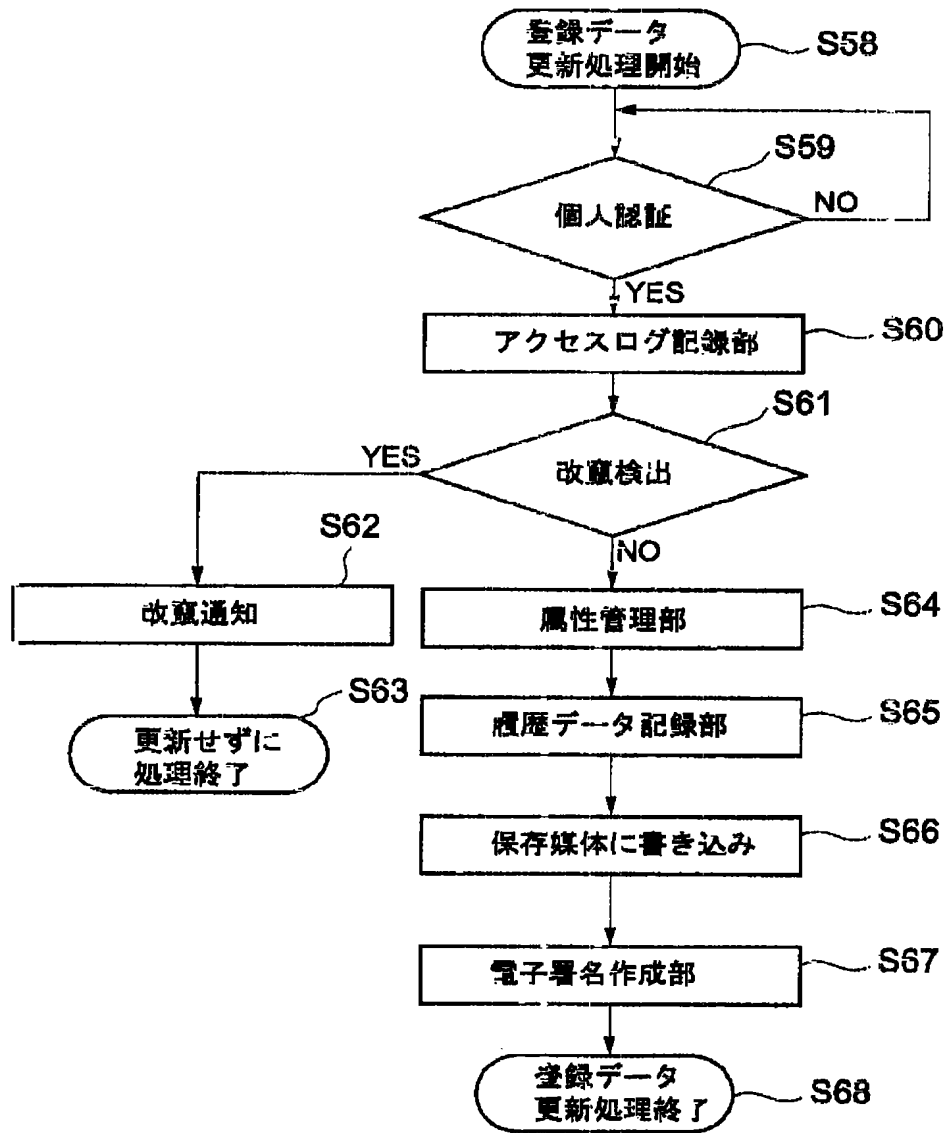
【図16】



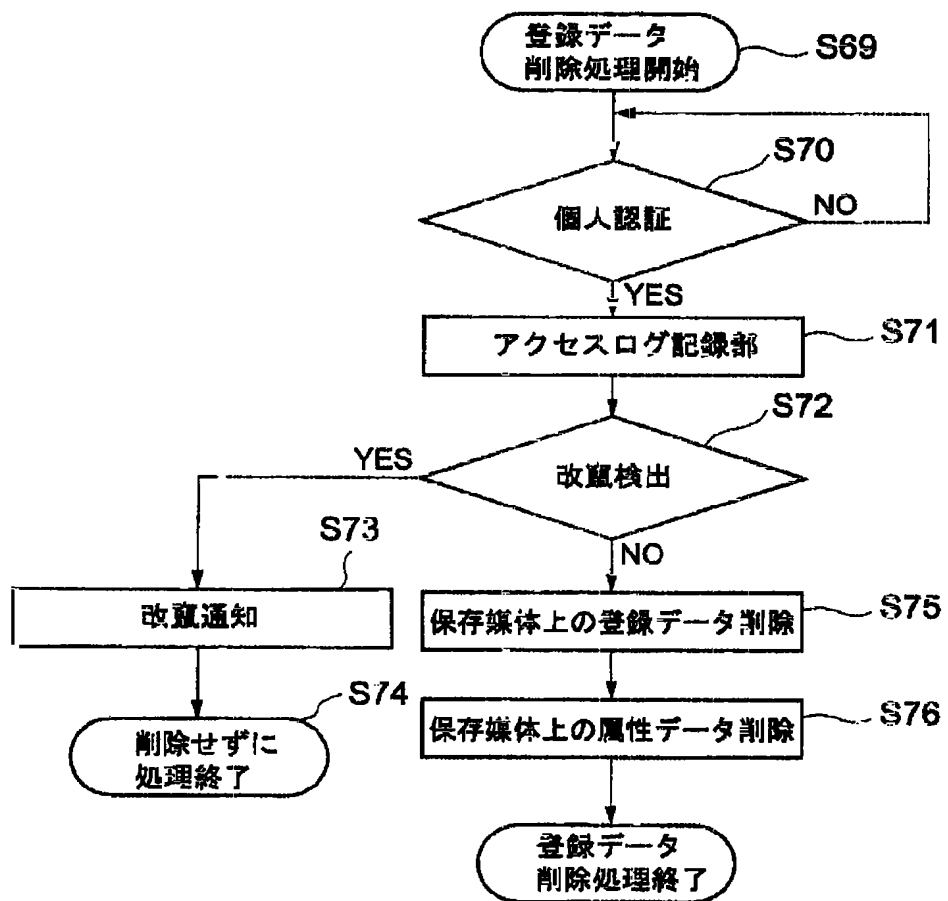
【図18】



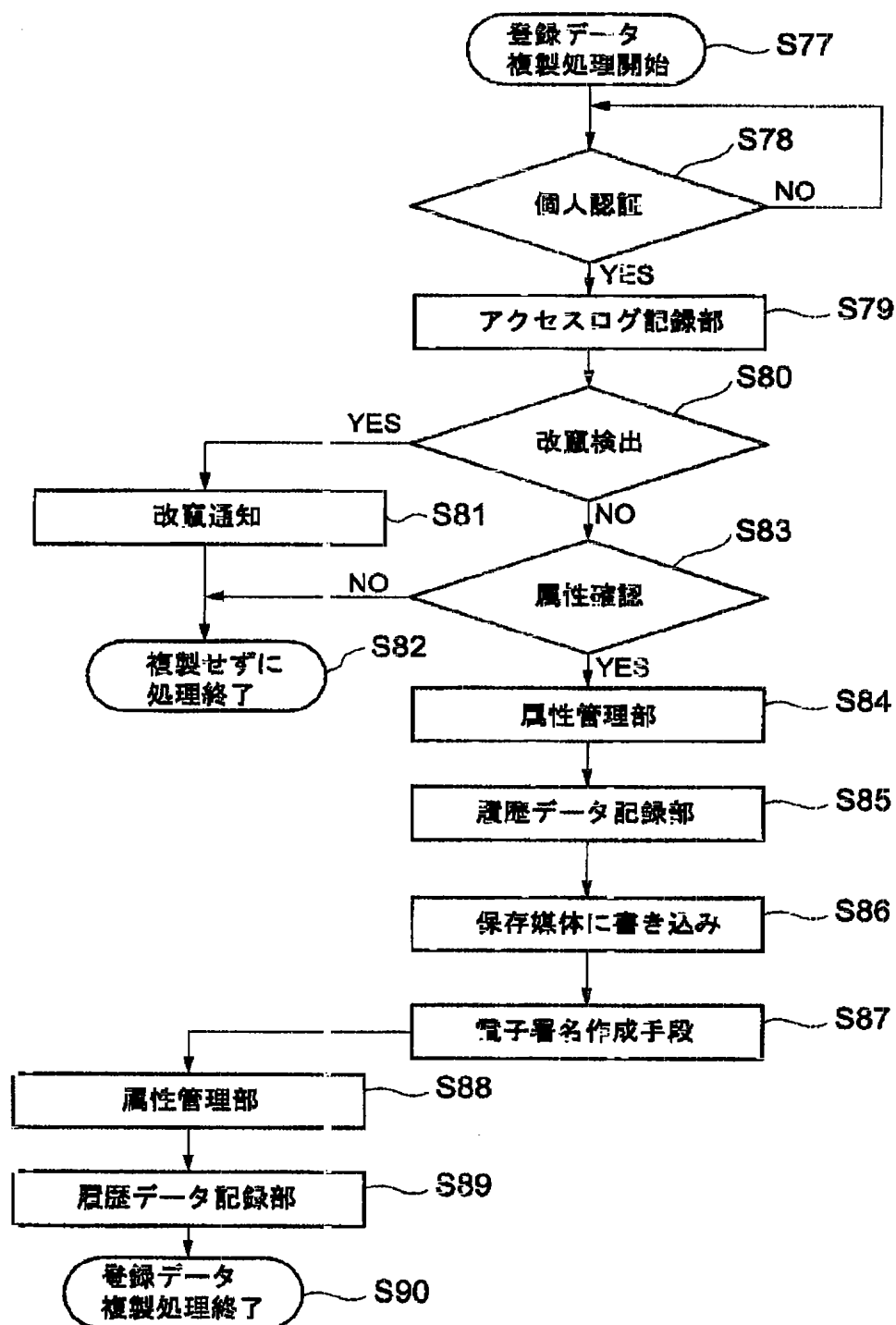
【図19】



【図20】



【図21】



【手続補正書】

【提出日】平成12年7月18日(2000.7.18)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項3

【補正方法】変更

【補正内容】

【請求項3】前記計算機本体に備えられた処理部にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行うことを特徴とする請求項1記載のデジタルデータ記録再生システム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】請求項8

【補正方法】変更

【補正内容】

【請求項8】前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用コードと、を照合する照合部とを備えることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】請求項9

【補正方法】変更

【補正内容】

【請求項9】前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードと、を照合するための照合部とを備えることを特徴とする請求項1記載のデジタルデータ記録再生システム。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0004

【補正方法】変更

【補正内容】

【0004】このような問題を解決するため、近時、公表されている「原本性保証電子保存システムの開発」(創造的ソフトウェア育成事業及びエレクトリック・コマース推進事業に係る最終成果発表会1998)においては、2台の電子計算機をそれぞれ保存装置とホスト装置というように位置づけ、それらをLANなどのネット

ワークで接続して使用している。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正内容】

【0013】また、本発明によると、上記課題を解決するために、(3) 前記実行可否判定部は、前記計算機本体に備えられた処理部にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行うことを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正内容】

【0018】また、本発明によると、上記課題を解決するために、前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用コードと、を照合する照合部とを備えることを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正内容】

【0019】また、本発明によると、上記課題を解決するために、前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードと、を照合するための照合部とを備えることを特徴とする(1)記載のデジタルデータ記録再生システムが提供される。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0049

【補正方法】変更

【補正内容】

【0049】図3に示すように、実行可否判定部1は、前記計算機本体15に備えられている処理部17にあらかじめ格納されているホスト識別子16を取得することにより、前記制御部8による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0051

【補正方法】変更

【補正内容】

【0051】はじめに、実行可否判定部1は、前記計算機本体15に備えられている処理部17に対してホスト識別子取得要求を送信する。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0052

【補正方法】変更

【補正内容】

【0052】そして、処理部17では、実行可否判定部1からのホスト識別子取得要求を受信すると、実行可否判定部1に対してホスト識別子16を送信する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0054

【補正方法】変更

【補正内容】

【0054】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、前記計算機本体11に備えられた処理部17にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子16を読み出して判定を行なうことを特徴とするデジタルデータ記録再生システムが提供される。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0119

【補正方法】変更

【補正内容】

【0119】続いて、改竄検出部3（の照合部3a）は、計算された照合用コードと保存媒体13より読み出された電子署名25を復号化して得られる照合用コードとの照合を行う（ステップS30）。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0120

【補正方法】変更

【補正内容】

【0120】この場合、改竄検出部3（の照合部3a）は、計算された照合用コードと保存媒体13より読み出された電子署名25を復号化して得られる照合用コードとの両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0122

【補正方法】変更

【補正内容】

【0122】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部3は、前記計算機本体15に接続された保存部12の各データファイル（保存媒体13）に対して記録されている電子署名25を復号化して得られる照合用コードと、前記保存部12の各データファイル（保存媒体13）から所定の算出式に基づいて計算される照合用コードと、を照合する照合部3aとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0129

【補正方法】変更

【補正内容】

【0129】続いて、改竄検出部3（の照合部3a）は、この読み出されたデータ24に対する照合用コードを算出する（ステップS28）。

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0130

【補正方法】変更

【補正内容】

【0130】ここで、照合用コードはデータ24の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0131

【補正方法】変更

【補正内容】

【0131】そして、改竄検出部3（の照合部3a）は、照合用コードの算出が終了すると、I/O制御手段7を介して、保存媒体13にデータ24が書き込まれたときに、それと共に書き込まれている電子署名25を読み出して復号化する（ステップS29）。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0132

【補正方法】変更

【補正内容】

【0132】続いて、改竄検出部（の照合部3a）3は、計算された照合用コードと保存媒体13より読み出された電子署名25を復号化した照合用コードとの照合を行う（ステップS30）。

【手続補正19】

【補正対象書類名】明細書

【補正対象項目名】0133

【補正方法】変更

【補正内容】

【0133】この場合、改竄検出部（の照合部3a）3は、計算された照合用コードと保存媒体13より読み出された電子署名25を復号化した照合用コードとの両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】0136

【補正方法】変更

【補正内容】

【0136】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部3は、前記計算機本体15に接続された保存部12の各データファイルに対して記録されている電子署名を復号化した照合用コードと、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードとを照合するための照合部3aとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【手続補正21】

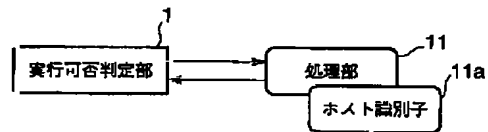
【補正対象書類名】図面

【補正対象項目名】図3

【補正方法】変更

【補正内容】

【図3】



【手続補正22】

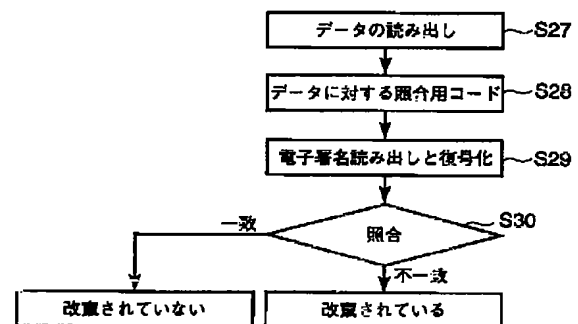
【補正対象書類名】図面

【補正対象項目名】図10

【補正方法】変更

【補正内容】

【図10】



フロントページの続き

Fターム(参考) 5C064 CC01 CC06  
 5D044 BC06 CC04 DE48 DE49 GK17  
 5J104 AA07 AA09 KA01 KA04 KA16  
 LA06 NA35 NA38  
 9A001 BB02 BB03 BB04 BB05 CC02  
 DD09 EE03 HH21 HH23 JJ08  
 JJ12 KK37 KK60 KZ16 LL03